**IN THE SPECIFICATION:**

The specification as amended below with replacement paragraphs and header shows added text with underlining and deleted text with ~~strikethrough~~.

Please REPLACE the paragraph beginning at page 6, line 13, with the following paragraph:

The encryption key when encrypting the use restriction information can be a password which is preset by the user, ID information inherent to a recording medium in which the synthetic data is recorded, or ~~vital~~ biometric information of the user.

Please REPLACE the paragraph beginning at page 11, line 14, with the following paragraph:

In addition, according to the present invention, there is provided a data administration method comprising the steps of: producing a real data section by encrypting digital content that conducts distribution; producing a header (summary) data section so as to visually and auditorily recognize the contents of the digital content; producing a consent information added ~~header~~ summary data section in which consent information containing the information of a contents key used as a encryption key when the digital content are encrypted is embedded in the ~~header~~ summary data section as a visually or auditorily unrecognizable electronic watermark; and allowing ~~vital~~ biometric template information produced on the basis of the ~~vital~~ biometric information of the user of the digital content to be held in the synthetic data, and distributing the synthetic data.

Please REPLACE the paragraph beginning at page 11, line 22, with the following paragraph:

The ~~vital~~ biometric template information can be embedded in the ~~header~~ summary data section as a visually and auditorily unrecognizable electronic watermark.

Please REPLACE the paragraph beginning at page 23, line 3 with the following paragraph:

In addition, as the user information 14 inherent to the user, the ~~vital~~ biometric information of the user can be used. For example, the fingerprint information, the retina information, the iris information, the voiceprint information of the user, etc., are registered at the contents manager 2 side in advance, and the contents key can be encrypted on the basis of the respective ~~vital~~ biometric information. For example, in the case where the contents key is encrypted by using the fingerprint information, the fingerprint image of the user is registered at the contents

manager 2 side in advance. The contents manager 2 side analyzes the fingerprint image of the user as registered, extracts the characteristics which is called "manusha" such as the end point or branch point of the fingerprint image, and encrypts the contents key by the characteristic information.

Please REPLACE the paragraph beginning at page 25, line 20 with the following paragraph:

The consent information 13 is encrypted by the encryption key based on the user information 14 and can be decoded by using the user information 14. In the case where the user information 14 is a password, the password is inputted by the user and the inputted password is used to decode the consent information 13. Also, in the case where the consent information is encrypted by the ID information of the information device such as the serial No. of the CPU, the serial No. of the media drive, and so on, the ID information of the information device presently used is obtained, and the consent information 13 is decoded on the basis of the ID information. In addition, in the case where the consent information is encrypted by the ~~vital~~ biometric information of the user, the ~~vital~~ biometric information of the user is inputted and then analyzed into the characteristic information caused by the end point, the branch point and so on, and the consent information is decoded by the characteristic information.

Please REPLACE the paragraph beginning at page 26, line 13 with the following paragraph:

If the password received from the user, the ID information of the information device presently used by the user, the characteristic information based on the ~~vital~~ biometric information received from the user, and so on are normal, the just contents key is restored from the consent information 13.

Please REPLACE the header at page 27, line 11 with the following header:

Certification Method due to ~~vital~~ biometric information

Please REPLACE the paragraph beginning at page 27, line 12 with the following paragraph:

The user who will use the digital content can conduct the certification of whether there is a just user or not by using the ~~vital~~ biometric information of the user. The ~~vital~~ biometric information may be the fingerprint information, the iris information, the retina information, the voiceprint information, and so on as described above. In this example, a case where the certification is conducted by using the fingerprint information will be described with reference to

Figs. 9 and 10.

Please REPLACE the paragraph beginning at page 31, line 24 with the following paragraph:

As described above, in the case where the consent information 13 is embedded in the ~~header~~ summary data section 16 as the invisible electronic watermark, the information on the embedding logic used when embedding the consent information 13 can be provided within the synthetic data 12. It is proposed that other than the consent information 13, ~~vital~~ biometric information on the user, the privileges information pertaining to the copyright and the like may be embedded as electronic watermark, and also it is proposed that the ~~vital~~ biometric information on the user, the privileges information pertaining to the copyright, the use information pertaining to the use term or the number of times of use of limit, and so on may be embedded in the digital content. If the kind of the embedding logic of the electronic watermark and the version information contained in the data section 16 and the real data section 15 are stored in the annex data section 17, respectively, the use at the contents user 3 side is facilitated. The operation will be described with reference to flowcharts shown in Figs. 12 and 13.